Responsible Disclosure GBLT

GBLT attaches a lot of value to the security of their IT-systems. Although countermeasures are taken to prevent intruders getting in. However, there is always a possibility for temporary vulnerabilities. When a vulnerability is found in our IT-systems, please report it within 24 hours. This will help to take adequate actions to fix this vulnerability. By reporting the vulnerability, you are accepting the terms that are written down in this 'Responsible Disclosure' . GBLT will handle your report with care, according the same terms.

GBLT asks the following:

- Report a vulnerability within 24 hours after detection.
    - Mail the findings to security@gblt.nl and use our public key, you can find in our attachment on our website.
- Provide the information needed to reproduce the error/vulnerability. In most cases an IP-address or URL of the affected system with a summary of the vulnerability is enough. In more complex vulnerabilities more information might be needed.
- Limit the findings to verifiable facts which are related to the vulnerability.
- Please provide us any tips that can help to fix the vulnerability. Avoid advertising for specific (security) products.
- Limit the findings to the outer layer of our network.
- Please leave a phone number so that we can contact you and work together for the best result. You are free to remain anonymous.
- Do not share the vulnerability to the public or other parties, even when the vulnerability can't be resolved in adequate time.
- Delete all the obtained data that has been exposed due to this vulnerability.

The following actions are not allowed:

- Do not download more data than necessary to test the leak. Also do not remove or change any data.
- Do not use 'tooling' that may cause nuisance to GBLT.
- Do not place malware on our systems
- Do not make use of 'Bruteforcing' to get access to our systems.
- Do not use 'Social engineering'.

GBLT promises you the following:

- We will respond within three working days to your report with our review and, if necessary, the expected solution term.
- We will keep you informed about the status of your report.
- We will treat your report confidentially and only provide your information to others if required by law.
- We will not communicate about your report in public and you will remain anonymous. Depending on the impact of the possible vulnerability, we might have to share the report with other involved parties.

- We will give a reward for a received unknown vulnerability report.
  The reward is based on the impact of a possible vulnerability and the completeness and usefulness of the report.